

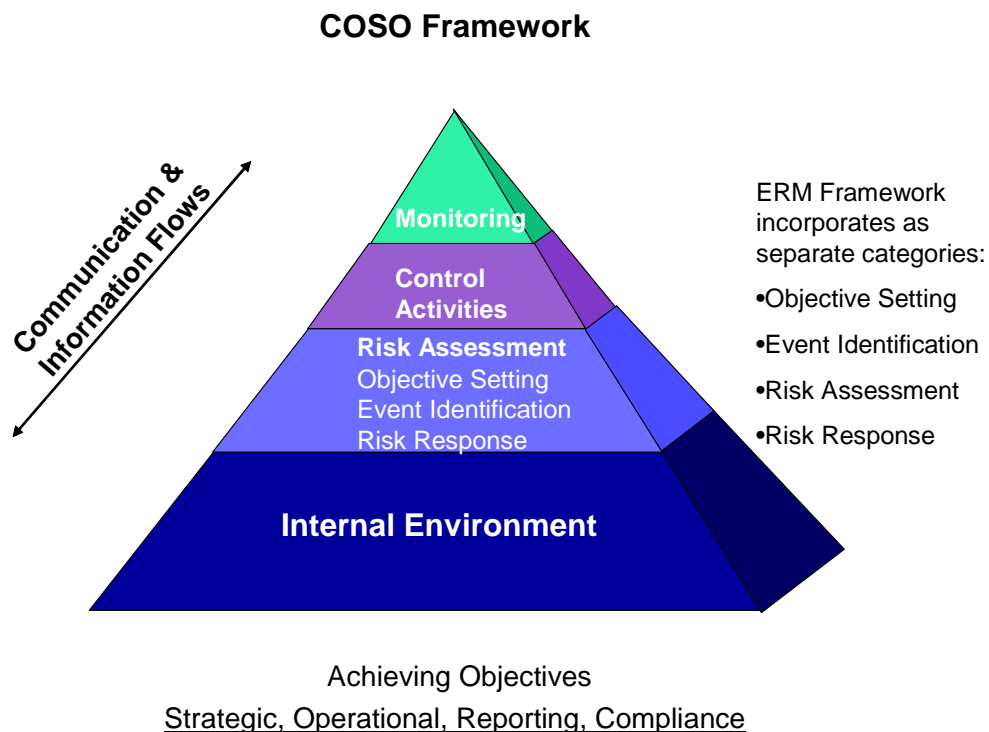
Control Framework

Management provides leadership and direction in achieving strategic and operational objectives that align with Texas A&M University's mission and vision of excellence. Operational activities are carried out in a highly regulated, complex, and constantly changing environment.

There is an integral relationship between achieving operational objectives, managing risks, and maintaining effective controls. Risks can have an adverse impact on the entity's ability to attain objectives. Operational activities can mitigate risks; and a control framework that is integrated in those activities spans the entity's culture, organizational structure, policies, processes and procedures, risk assessments, communication, and monitoring. An effective control framework reasonably ensures that:

- Strategic and operational objectives are achieved;
- Aims for workplace integrity and regulatory compliance responsibilities are met;
- Resources are used effectively and efficiently and protected from fraud, waste, and mismanagement; and
- Reliable and timely information is obtained, maintained, reported, and used by decision makers.

The following diagram illustrates a control framework based on COSO¹



¹ Concepts for the COSO Framework diagram are taken, in part, from the Committee of Sponsoring Organizations of the Treadway Commission (COSO): *Internal Control - Integrated Framework* and the *Enterprise Risk Management - Integrated Framework*.

COSO Framework Components

Internal Environment is the organizational culture that influences ethical behavior, workplace integrity, and risk and compliance consciousness of its personnel. It includes organizational structure; formal rules and procedures; delegation of authority and responsibility; incentives and rewards; and human resource management, including commitment to personnel competency.

Risk Assessment is the process of identifying risk events or incidents that threaten the organization's achievement of objectives, mapping activities that mitigate risks, and developing risk management responses that are aligned with the entity's appetite or tolerance to risks. Enterprise risk management addresses risks from an entity-wide perspective.

Control Activities are those activities, e.g., authorizations, analytical reviews, verifications, reviews of operating performance, etc., established to help see that compliance requirements and risk responses selected by management are effectively carried out. Mitigating activities that limit risks rely largely on a system of controls that are integrated in operations.

Communication and Information Flows are critical in clarifying expectations and providing the right information to the right people at the right time for them to effectively carry out their responsibilities. Useful information has relevant content and is timely, current, accurate, and accessible.

Monitoring verifies that controls are working as intended and identifies anomalies. Monitoring is done at various organizational levels to include: check points by personnel performing daily tasks; reviews of transactions or events by supervisors; spot checks by objective individuals; and various reviews by peers, management advisory services, consultants, and auditors.

COSO Framework - System of Controls

The concept of a system of controls is reflected in how controls collectively manage risks.

- Preventive controls protect against risks before they happen. Examples include, employee screening, documented approvals, segregation of duties, restricting access to automated systems and data, and physically securing cash, equipment, etc.
- Detective controls identify risk events or incidents soon after they occur. Examples include supervisory review of transactions, timely reconciliations, review of exception reports, segregation of duties, and comparison of actual to expected results.
- Certain controls deter risks of non-compliance and misconduct. Examples include incentives, expanded communication, required training, consistently holding personnel accountable and disciplining, as necessary, and outside reviews and audits.

The cost/benefit, acceptable level of risk, and contribution within the overall control framework are important in selecting specific controls. Also important is the nature of the activity, including susceptibility to errors and fraud. An effective control framework manages risks and supports planning, stewardship, compliance, and informed decisions that help management achieve operational objectives.